ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 306 (2006) 201–207

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

A subgroup of SO(3, ℝ) generated by rotations of orders 4 and 8

Geoffrey R. Robinson

Department of Mathematical Sciences, University of Aberdeen, Aberdeen, AB 24 3UE, Scotland, UK

Received 19 December 2005

Available online 30 May 2006

Communicated by Richard Dipper, Martin Liebeck and Andrew Mathas

Dedicated to Gordon James on the occasion of his 60th birthday

Abstract

We prove that a subgroup of the real 3-dimensional special orthogonal group generated by a pair of rotations of respective orders 4 and 8 (belonging to a family of such groups considered by Radin and Sadun in [C. Radin, L. Sadun, On 2-generator subgroups of $SO(3)$, Trans. Amer. Math. Soc. 351 (1999) 114469–114480]) has an epimorphic image which is one of $\mathrm{PSL}(2, p)$, $\mathrm{PSL}(2, p^2)$, $\mathrm{PGL}(2, p)$ or $\mathrm{PGL}(2, p^2)$ (depending on the congruence of p (mod 16)) for all odd primes p, by considering its reduction (mod p) as a linear group.

1. Introduction

In [2], Radin and Sadun determined the structure of certain subgroups of $\mathrm{SO}(3, \mathbb{R})$ generated by a pair of rotations of finite order whose axes of rotation are at an angle which is a rational multiple of π. The essential case is when the axes of rotation are orthogonal, and the case that one of the rotations has order 4 is especially critical. With few explicit exceptions when the groups are finite, such groups are described as free products with amalgamation over common subgroups of pairs of groups which are either all cyclic, dihedral (including Klein 4-groups), or S_4, the symmetric group of degree 4.

In this paper, we will study the behavior of these groups under reduction (mod p), which is available for all odd primes p. We will only consider the case that the two axes of rotation

E-mail address: g.r.robinson@abdn.ac.uk.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.04.034

are orthogonal, and (deviating from the notation of [2]), we will denote by $G_{(m,n)}$ the group generated by

$$x_m = \begin{pmatrix} \cos(\frac{2\pi}{m}) & \sin(\frac{2\pi}{m}) & 0 \\ -\sin(\frac{2\pi}{m}) & \cos(\frac{2\pi}{m}) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and

$$y_n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ 0 & -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}$$

for positive integers m and n. We will be particularly interested in the group $G_{(4,8)}$.

We summarize here (some of) the results of [2]: as usual, for groups A and B with a common subgroup C, the notation $A *_C B$ is the free product of A and B amalgamated over C (if C is omitted, then the product is just the free product of A and B). We also use D_n to denote the dihedral group of order n (that is, with $2n$ elements) and D_2 to denote the Klein 4-group.

Theorem. (Radin and Sadun [2])

(i) *If m is odd, we have $G_{(m,4)} \cong D_m *_{\mathbb{Z}_2} \mathbb{Z}_4$.*
(ii) *If m is even, but not divisible by 4, then we have $G_{(m,4)} \cong D_m *_{D_2} D_4$.*
(iii) *If $4|m$, then $G_{(m,4)} \cong D_m *_{D_4} S_4$.*
(iv) *If p and q are both odd, then $G_{(p,q)} \cong \mathbb{Z}_p * \mathbb{Z}_q$.*
(v) *If p is even and q is odd, then $G_{(p,q)} \cong \mathbb{Z}_p *_{\mathbb{Z}_2} D_q$.*
(vi) *If p, q are both even, but q is not divisible by 4, then $G_{p,q} \cong D_p *_{D_2} D_q$.*
(vii) *If p and q are both divisible by 4, then we have $G_{(p,q)} \cong G_{(\mathrm{lcm}(p,q),4)}$, so this group may also be expressed as a free product with amalgamation, as in part* (iii).

We remark here that while (with the noted exceptions) the groups involved are infinite, and the representations as given are not realized over a ring of algebraic integers, it is still possible to perform the process of reduction (mod p) for all odd primes p (but it is not possible to perform reduction (mod 2), since it is easy to check that trace$(x_m y_n)$ has negative valuation at all prime ideals containing the rational prime 2 (of the relevant ring of cyclotomic integers)).

When nm is divisible by p, we will see that the reduction (mod p) of $G_{(m,n)}$ depends only on the "smaller" pair of integers $(m_{p'}, n_{p'})$. As usual, for a positive integer n and a prime p, we have set $n_p = p^{v_p(n)}$ and $n_{p'} = \frac{n}{n_p}$.

We note that $\langle x_4, y_4 \rangle \cong S_4$, and that $(x_4 y_4)^2$ has order 3. Furthermore, $x_2 = x_4^2$ inverts y_8 and y_2 inverts x. Notice also that (using [2]) $\langle x_2, y_8 \rangle$ and $\langle x_4, y_4 \rangle$ are maximal finite subgroups of G.

Theorem 1. *G has epimorphic images as follows for odd primes p*:

(i) PSL$(2, p)$ *whenever* $p \equiv \pm 1 \pmod{16}$.
(ii) PGL$(2, p)$ *whenever* $p \equiv \pm 7 \pmod{16}$.
(iii) PGL$(2, p^2)$ *whenever* $p \equiv \pm 3 \pmod{8}$.

Moreover, the epimorphisms may be chosen so that each has torsion free kernel and so that the intersection of the kernels of any infinite number of them is trivial. Also, G has no non-identity solvable normal subgroup and $[G : G'] = 2$.

Remark. In various private communications since January 2006, J.-P. Serre has provided us with a proof that $G_{(4,8)} \cong \mathrm{SO}(3, \mathbb{Z}[\frac{1}{\sqrt{2}}])$, which may be viewed as a strengthening of the above theorem, and has also provided examples to illustrate that, even in the cases when $G_{(m,n)}$ is infinite, it is not always the case that $G_{(m,n)}$ is the full special orthogonal group over the ring generated by the traces of its elements.

1.1. On the groups $G_{(m,n)}$

We note that for positive integers m and n both greater than 2, the group $G_{(m,n)}$ is an absolutely irreducible linear group. For, in that case (after extending scalars to $\mathbb{C}$), all eigenspaces of x_m and y_n are 1-dimensional and x_m and y_n have no common eigenvector. On the other hand, if the representation were reducible (over $\mathbb{C}$), then (since the matrices are orthogonal) there would be an invariant 1-dimensional subspace, and hence x_m and y_n would have a common eigenvector.

We note for future use that x_2 inverts each y_n and centralizes each x_n, while y_2 inverts each x_n and centralizes each y_n. Hence the Klein 4-group $G_{(2,2)} = \langle x_2, y_2 \rangle$ normalizes each of the groups $G_{(m,n)}$.

When $\min(m, n) \leqslant 2$, it is clear that $G_{(m,n)}$ is reducible, while $G_{(m,n)}$ is a finite dihedral group when the minimum is 2 (including the possibility of a Klein 4 group). We note that (for a given choice of m and n), we have $G_{(m,n)} \leqslant G_{(rm,sn)}$ for all positive integers r and s. If a, b, c, d are positive integers with $\gcd(a, c) = \gcd(b, d) = 1$, then $G_{(ac,bd)} = \langle G_{(a,b)}, G_{(c,d)} \rangle$. In that case, we note in particular that $G_{(a,b)} \lhd G_{(ac,bd)}$ if $\{c, d\} \subseteq \{1, 2\}$.

1.2. Reduction (mod p)

Now let us fix a choice of $G_{(m,n)}$ and an odd prime p. Let $d(m, n) = \mathrm{lcm}(4, m, n)$, and let $\omega = e^{2\pi i/d(m,n)}$. Let ρ be a prime ideal of $\mathbb{Z}[\omega]$ containing p. Let R denote the localization $\mathbb{Z}[\omega]_\rho$ and ρ^* denote the unique maximal ideal of R. Let F denote R/ρ^*. We note that $\cos(\frac{2\pi}{n})$, $\cos(\frac{2\pi}{m})$, $\sin(\frac{2\pi}{n})$, $\sin(\frac{2\pi}{m})$ all lie in R, since 2 is a unit of R. We let $G_{(m,n),\rho}$ denote the image of $G_{(m,n)}$ under the natural epimorphism from $\mathrm{SO}(3, R)$ to $\mathrm{SO}(3, F)$. We refer to $G_{(m,n),\rho}$ (somewhat loosely) as a reduction (mod p) of $G_{(m,n)}$. We note that the field F so obtained, and the images of x_m and y_n in $\mathrm{SO}(3, F)$, only depend on the integers $m_{p'}$ and $n_{p'}$. This is because $1 - \zeta \in \rho$ whenever ζ is a $d(m, n)$th root of unity whose order is a power of p, so that $\cos(\frac{2\pi}{n}) \equiv \cos(\frac{2\pi}{n_{p'}}) \pmod{\rho^*}$ (and similarly for sin).

We also note that the group $G_{(m,n),\rho}$ is absolutely irreducible whenever $\min(m_{p'}, n_{p'}) \geqslant 3$ (and is reducible otherwise). For, if $G_{(m,n),\rho}$ were reducible (after extension of scalars to an algebraically closed field) then we claim that there would be a 1-dimensional invariant subspace. If not, there is a 2-dimensional invariant subspace, say W. However, the 1-dimensional orthogonal complement, $W^\perp$, of W (which may be contained in W) is also invariant, since $G_{(m,n)} \subseteq \mathrm{SO}(3, F)$. In that case, the images of x_m and y_n would have a common eigenvector, which they do not, as in the complex case.

We remark that $G_{(m,n)}$ embeds in the direct product of any infinite collection of $G_{(m,n),\rho}$'s. In fact, since there are infinitely many primes p congruent to 1 (mod $d(m, n)$), we could also

embed $G_{(m,n)}$ in the direct product of any infinite collection of SO(3, p)'s, as p ranges through such (distinct) primes.

Remark. For the group $G_{(4,8)}$ and an odd prime p, we do not need to pass to such a large degree extension as in the previous section to perform reduction (mod p). For example, when $p \equiv \pm 1$ (mod 8), we know that 2 is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$, and it follows that $\sqrt{2}$ exists (and is a unit) in the (complete) p-adic integers $\mathbb{Z}_p$. Hence we may embed the group $G_{(4,8)}$ in $\mathrm{SO}(3, \mathbb{Z}_p)$ and obtain a natural homomorphism to SO(3, p). When $p \equiv \pm 3$ (mod 8), we can view $G_{(4,8)}$ as a subgroup of $\mathrm{SO}(3, \mathbb{Z}_p[\sqrt{2}])$, and obtain a natural homomorphism to SO(3, p^2). In the latter case, since $\mathrm{trace}(y_8) = 1 + \sqrt{2}$, the resulting image cannot be realized (even up to equivalence) as a subgroup of GL(3, p), as the trace of the representation does not take values in GF(p). For any odd prime p, we denote the resulting image by $G_{(4,8),p}$.

2. The group $G_{(4,8)}$

We recall from the theorem of Radin and Sadun that $G_{(4,4n)} = G_{(4n,4n)}$ for each positive integer n. In fact, a direct calculation shows that $(y_4x_4)y_{4n}(y_4x_4)^{-1} = x_{4n}$, so that x_{4n} and y_{4n} are conjugate in $G_{(4n,4n)}$. In particular, we have $G_{(4,8)} = G_{(8,8)}$.

We remind the reader that when F is a finite field of odd characteristic, $\mathrm{PGL}(2, F) \cong \mathrm{SO}(3, F)$. To see this, let GL(2, F) act by conjugation on 2×2 matrices of trace 0 (with entries in F), and observe that the non-degenerate symmetric bilinear form $\langle a, b\rangle = \mathrm{trace}(ab)$ is invariant under this action. This illustrates that the derived group of SO(3, F) has index 2, and is generated by the elements whose eigenvalues λ all satisfy $\lambda^{\frac{|F|-1}{2}} = 1$ if $\lambda \in F$ and $\lambda^{\frac{|F|+1}{2}} = 1$ if $\lambda \notin F$. For $[\mathrm{PGL}(2, F) : \mathrm{PSL}(2, F)] = 2$, and the elements of $\mathrm{PGL}(2, F) \setminus \mathrm{PSL}(2, F)$ are the images of those matrices in GL(2, F) whose determinants are non-squares in F.

We need to examine subgroups of GL(2, p) and GL(2, p^2) in some detail for odd primes p. It is well known that a subgroup of GL(2, p) which has more that one Sylow p-subgroup contains SL(2, p). Similarly, it is easy to check that any subgroup of GL(2, p^2) which has more that one Sylow p-subgroup contains a subgroup isomorphic to SL(2, p). We prove:

Lemma 2. *Let p be a prime congruent to* ± 3 (mod 8). *Let H be a subgroup of* GL(2, p^2) *which has more than one Sylow p-subgroup, and which contains an element t of order* 8 *with eigenvalues* 1 *and* ω. *Then H contains* SL(2, p^2) *and H maps onto* PGL(2, p^2) *under the natural projection.*

Proof. Since $p \equiv \pm 3$ (mod 8), we have $p^2 \equiv 9$ (mod 16), so that $\frac{p^2-1}{8}$ is odd and GF(p^2) contains no element of multiplicative order 16. Let $L = O^{p'}(H) \leqslant \mathrm{SL}(2, p^2)$. It suffices to prove that $p^2 \mid |L|$, for distinct Sylow p-subgroups of SL(2, p^2) have trivial intersection and L has more than one Sylow p-subgroup. Hence, in that case, we see that L contains $p^2 + 1$ Sylow p-subgroups. Since SL(2, p^2) is generated by its $p^2 + 1$ Sylow p-subgroups, we then obtain $L = \mathrm{SL}(2, p^2)$. Also, by assumption, H contains an element (namely t, of order 8) whose determinant is not a square in the field of p^2 elements, so $H/(H \cap Z(\mathrm{GL}(2, p^2))) = \mathrm{PGL}(2, p^2)$.

We remark that the hypotheses imply that H is absolutely irreducible as a linear group. Let $P \in \mathrm{Syl}_p(L)$, and let us note that $O^p(C_H(u)) = Z(H)$ for each non-identity element $u \in P$. Now $H = LN_H(P)$ and we may write $t = sz$ for some $s \in L$ and $z \in N_H(P)$. Then $\det(z) = \omega$ and we may suppose that z is a 2-element.

Since the 1-dimensional fixed-point space of P is z-invariant, we see that both eigenvalues of z are in $\mathrm{GF}(p^2)$. Hence both eigenvalues of z are 8th roots of unity, and z itself has order 8. Let the eigenvalues of z be ω^j and ω^{9-j} where $j \in \{1, 3, 5, 7\}$. Then the eigenvalues of z^4 are -1 and 1, since $9 - j$ is even. In particular, z^4 is non-scalar, so that $zC_H(P)$ has order 8 in $N_H(P)/C_H(P)$. Thus P is not cyclic, as $p \equiv \pm 3 \pmod 8$, and the lemma is proved. □

Theorem 3. *Let $G_{(m,n),\rho}$ be a reduction* (mod p) *constructed as before, where p is an odd prime. Suppose that* $\min(n_{p'}, m_{p'}) \geqslant 3$. *Then* (*except for the case* $(m_{p'}, n_{p'}) = (4, 4)$)*, the group $G_{(m,n),\rho}$ has order divisible by p and is an absolutely irreducible and primitive linear group.*

Proof. If mn is odd, then $G_{(m,n)} \lhd G_{(2m,2n)}$, while if m is odd but n is even, then $G_{(m,n)} \lhd G_{(2m,n)}$. In each case, the factor group has order dividing 4.

Suppose then that we can establish that $G_{(m',n'),\rho}$ is (absolutely) primitive of order divisible by p, where $m' = \mathrm{lcm}(m, 2)$ and $n' = \mathrm{lcm}(n, 2)$. In that case, it would certainly be the case that $G_{(m,n),\rho}$ would have order divisible by p, since p is odd. If $G_{(m,n),\rho}$ were imprimitive (even over an extension field), then it would have an Abelian normal subgroup with factor group isomorphic to a subgroup of S_3. In particular, $G_{(m,n),\rho}$ would be solvable.

However, the Fitting subgroup $F = F(G_{(m,n),\rho})$ is normal in $G_{(m',n'),\rho}$, so $Z(F)$ is normal in $G_{(m',n'),\rho}$, and then central, by primitivity. Thus $Z(F)$ consists of scalars, by absolute irreducibility. However, each element of $G_{(m',n'),\rho}$ has an eigenvalue 1, so that $Z(F) = 1$ and then $F = 1$. But $G_{(m,n),\rho}$ is solvable and non-trivial, a contradiction.

Hence it suffices to consider the case that $m_{p'}$ and $n_{p'}$ are both even. Suppose that $m_{p'}$ and $n_{p'}$ are both at least 6. Suppose further that $G_{(m,n),\rho}$ has order prime to p. Then it "lifts" to an absolutely irreducible p'-subgroup, say X, of $\mathrm{GL}(3, \mathbb{C})$ with Brauer character (at a given element u) uniquely determined by the eigenvalues of the corresponding element of $G_{(m,n),\rho}$. In particular, X contains (non-central) elements of orders $m_{p'}$ and $n_{p'}$ with eigenvalues 1, $e^{2\pi i/m_{p'}}$, $e^{-2\pi i/m_{p'}}$ and 1, $e^{2\pi i/n_{p'}}$, $e^{-2\pi i/n_{p'}}$. A theorem of Blichfeldt [1] asserts that the element g of a finite primitive complex irreducible linear group Y is central in Y if there is an eigenvalue λ of g such that all eigenvalues of g are within $\frac{\pi}{3}$ of λ on S^1. Hence X is imprimitive, and the associated complex representation of $G_{(m,n),\rho}$ is equivalent to one induced from a 1-dimensional representation of a subgroup, H say, of index 3. The same is true (up to equivalence, and possibly over an extension field) for the given characteristic p representation of $G_{(m,n),\rho}$.

Let w_m be the image of x_m and z_n denote the image of y_n in $G_{(m,n),\rho}$. But no sum of eigenvalues of w_m is 0 in R/ρ^* (for example, if $1 + \theta + \theta^{-1} = 0$, then $\theta^3 = 1$, whereas the eigenvalues of w_m are roots of unity of order at least 6). It follows by Mackey's theorem that w_m is in $\mathrm{core}_X(H)$. A similar argument applies to z_n. But then w_m and z_n commute, and $G_{(m,n),\rho}$ is Abelian, a contradiction, as it is an absolutely irreducible linear group. Hence p divides the order of $G_{(m,n),\rho}$ (and $G_{(m,n),\rho}$ is an absolutely primitive linear group).

We are left to consider the case $m_{p'} = 4, n_{p'} \geqslant 6$. If the given representation of $G_{(m,n),\rho}$ is equivalent (possibly over an extension field) to one induced from a 1-dimensional representation of a subgroup of index 3, say H, then z_n lies in $K = \mathrm{core}_{G_{(m,n),\rho}}(H)$. Since $G_{(m,n),\rho}/K$ is isomorphic to a subgroup of S_3 we see also that w_m^2 lies in K. Thus $[y_n, x_2] = y_{\frac{n}{2}}$ lies in the kernel of the natural epimorphism from $G_{(m,n)}$ to $G_{(m,n),\rho}$. This is a contradiction, since the p'-part of y_n has order at least 4, and the p'-part of z_n has the same order. □

Proof of Theorem 1. We will prove that $G_{(4,8),p} \cong \mathrm{PSL}(2, p)$ whenever $p \equiv \pm 1 \pmod{16}$, that $G_{4,8,p} \cong \mathrm{PGL}(2, p)$ whenever $p \equiv \pm 7 \pmod{16}$, and that $G_{4,8,p} \cong \mathrm{PGL}(2, p^2)$ whenever $p \equiv \pm 3 \pmod 8$.

Since $G_{(4,8),p}$ acts (absolutely) irreducibly in characteristic p, it has no non-trivial normal p-subgroup. By Theorem 3, $G_{(4,8),p}$ has order divisible by p (and has more than one Sylow p-subgroup, since it is irreducible).

In the case that $p \equiv \pm 1 \pmod 8$, we know that $G_{(4,8),p}$ is a subgroup of $\mathrm{SO}(3, p)$ ($\cong \mathrm{PGL}(2, p)$). Since $G_{(4,8),p}$ has more than one Sylow p-subgroup, it contains (a normal subgroup of index at most 2 isomorphic to) $\mathrm{PSL}(2, p)$.

The eigenvalues (other than 1) of the images of x_4 and y_8 are, respectively, primitive 4th and 8th roots of unity. If $8 \mid p - 1$, then the image will contain an element of $\mathrm{PGL}(2, p) \setminus \mathrm{PSL}(2, p)$ exactly when a primitive 8th root of unity is not a square in $\mathrm{GF}(p)$, that is, when $p \equiv 9 \pmod{16}$. If $8 \mid p + 1$, then the image contains an element of $\mathrm{PGL}(2, p) \setminus \mathrm{PSL}(2, p)$ only when a primitive 8th root of unity $\zeta \in \mathrm{GF}(p^2)$ does not satisfy $\zeta^{\frac{p+1}{2}} = 1$, that is, precisely when $p \equiv 7 \pmod{16}$.

In the case that $p \equiv \pm 3 \pmod 8$, we know that $G_{(4,8),p}$ is a subgroup of $\mathrm{SO}(3, p^2) \cong \mathrm{PGL}(2, p^2)$ which has more than one Sylow p-subgroup. The image of y_8 in $\mathrm{SO}(3, p^2)$ is also the image in $\mathrm{SO}(3, p^2)$ under the natural homomorphism from $\mathrm{GL}(2, p^2)$ of an element of order 8 which has an eigenvalue 1. By Lemma 2, we see that $G_{(4,8),p} \cong \mathrm{PGL}(2, p^2)$ in these cases.

For each odd prime p, the epimorphic image $G_{(4,8),p}$ lies between a certain non-Abelian simple group $\mathrm{PSL}(2, q)$ and its automorphism group, so it has no non-trivial solvable normal subgroup. Hence any solvable normal subgroup of $G_{(4,8)}$ is in the kernel of every reduction (mod p), so is trivial.

The principal ideal (p) remains prime in $\mathbb{Z}_p[\sqrt{2}]$ when $p \equiv \pm 3 \pmod 8$ (and (p) is certainly prime in $\mathbb{Z}_p$ when $p \equiv \pm 1 \pmod 8$). By the usual argument, if $g \neq I$ is an element of finite prime order with $g \equiv I_3 \pmod{p^k}$ (entrywise), but $g \not\equiv I_3 \pmod{p^{k+1}}$, then $g^{p^s} \equiv I_3 \pmod{p^{k+s}}$ but $g^{p^s} \not\equiv I_3 \pmod{p^{k+s+1}}$, for each positive integer s. If g has order prime to p, then we can choose arbitrarily large values of s for which $g^{p^s} = g$, a contradiction, since $g \neq I$. If $g^p = I$, then we evidently have a contradiction.

Since $G = G_{(4,8)}$ is generated by two conjugate elements of order 8, namely x_8 and y_8, we know that G/G' is generated by $y_8 G'$. But $x_2 = x_4^2$ inverts y_8, so that $[x_2, y_8] = y_8^2 \in G'$. Hence $[G : G'] \leqslant 2$. However, we know that $G_{(4,8)}$ has a homomorphic image of order 2, since (for example), it has $\mathrm{PGL}(2, 9)$ as a homomorphic image, which itself in turn has a factor group of order 2. □

Remark. With a little more effort, it is possible to prove in general (using a well-known theorem of L.E. Dickson) that $G_{(m,n),\rho}$ contains $\mathrm{PSL}(2, F)$ where F is the field generated by the traces of its elements, whenever $(4, 4) \neq \min(m_{p'}, n_{p'}) \geqslant 3$.

Acknowledgments

The author thanks Jean-Pierre Serre for many helpful communications about this work, which played a significant role in shaping this revised version and, in particular, for making us aware of the work of Radin and Sadun. It is also a pleasure to acknowledge helpful discussions related to this work with J. Kedra and C. Maclachlan (both of the University of Aberdeen).

References

[1] H. Blichfeldt, Finite Collineation Groups, Univ. of Chicago Press, 1917.
[2] C. Radin, L. Sadun, On 2-generator subgroups of $SO(3)$, Trans. Amer. Math. Soc. 351 (1999) 114469–114480.